Linear Codes over $\mathbb{Z}/(2^k)$ of Constant Euclidean Weight

Jay A. Wood
Department of Mathematics, Computer Science & Statistics
Purdue University Calumet
Hammond, Indiana 46323–2094
wood@calumet.purdue.edu

ABSTRACT. Carlet [**3**] determined the linear codes over $\mathbb{Z}/(2^k)$ of constant Lee weight. This paper describes a different approach to this problem, along the lines of [**6**], which we apply to determining the linear codes over $\mathbb{Z}/(2^k)$ of constant Euclidean weight.

1. Introduction

Over finite fields, any linear code with constant Hamming weight is a replication of simplex (i.e., dual Hamming) codes. There are several proofs of this result, including [**1**], [**5**], and [**6**]. Recently, Carlet [**3**] proved a similar result for linear codes of constant Lee weight over $\mathbb{Z}/(2^k)$.

In this work we generalize the approach of [**6**]. While more complicated than Carlet's proof, our approach applies to any weight function (Hamming, Lee, Euclidean, etc.). For the purposes of this paper, we will concentrate on the cases of Lee and Euclidean weight over the ring $\mathbb{Z}/(2^k)$. A more thorough discussion of the general situation will appear elsewhere.

Any linear code over a ground ring R can be viewed as an abstract R-module equipped with a linear embedding into R^n. The embedding is given by n coordinate functionals, i.e., by n linear functionals on C.

If a linear code has constant weight, Ward's key observation in [**6**, Theorem 4] was that the coordinate functionals consist of a union of orbits of the automorphism group of C acting on the space of linear functionals on C. This observation depends on the extension theorem [**7**] and appears as Theorem 9 of Section 5. Thus a linear code of constant weight is completely determined by its orbit multiplicities, the number of times an orbit appears in the collection of coordinate functionals.

The constant weight condition imposes equations on the orbit multiplicities. These equations are studied in Section 6. Theorem 13 shows that there always exists a one-dimensional rational space of solutions, hence a minimal integral solution. The only problem is that the integral solution could possibly have some negative coefficients. In fact, negative coefficients do not occur for Lee or Euclidean weights over $\mathbb{Z}/(2^k)$. This is proved in Theorems 14 and 15 of Section 7, where explicit descriptions of constant weight linear codes are given.

Partially supported by Purdue University Calumet Scholarly Research Awards.
August 23, 1999.

Throughout this paper, the ground ring will be $R = \mathbb{Z}/(2^k)$. It will be convenient to take representatives for $\mathbb{Z}/(2^k)$ from the set

$$\{t \in \mathbb{Z} : -2^{k-1} < t \leq 2^{k-1}\}. \tag{1}$$

A *linear code* C of length n is a submodule of R^n.

The *Lee weight* $w(x)$ of any element $x = (x_1, \ldots, x_n) \in R^n$ is defined to be

$$w(x) = \sum_{i=1}^{n} a_{x_i}, \tag{2}$$

where $a_t = |t|$, with $t \in R$ represented as in (1). Similarly, the *Euclidean weight* uses $a_t = |t|^2$. We will denote both types of weight by $w(x)$; the context will make clear which is being discussed.

REMARK 1. In the literature there are two different notions of Euclidean weight on the rings $\mathbb{Z}/(m)$. In the first notion, one embeds $\mathbb{Z}/(m)$ into $\mathbb{C}$ as the mth roots of unity and measures weight and distance using the squared Euclidean weight and distance inherited from $\mathbb{C}$. Thus, for $t \in \mathbb{Z}/(m)$, $a_t = |\exp(2\pi it/m) - 1|^2 = 2 - 2\cos(2\pi t/m)$. When $m = 4$, this version of Euclidean weight equals twice the Lee weight, [**4**, §IIC].

The second notion of Euclidean weight is the one described above, where $a_t = |t|^2$. One reason for the interest in this notion is the quotient map $\mathbb{Z} \to \mathbb{Z}/(m)$. Codes over $\mathbb{Z}/(m)$ pull back to lattices, and the minimum norm of vectors in the lattice is related to the minimum Euclidean weight of the code; see [**2**, §I].

The approach of this work towards linear codes of constant weight applies equally well to both notions of Euclidean weight. In this paper, we have chosen to concentrate on the second notion.

We wish to determine the linear codes of *constant weight*, i.e., codes for which there exists $L > 0$ with $w(x) = L$ for all nonzero $x \in C$. As above, $w(x)$ refers to a fixed choice of either Lee or Euclidean weight.

3. Examples

Before we proceed to discuss the theoretical underpinnings of this problem, let us present a few examples. The examples are given in terms of generator matrices. The linear code is obtained by forming all R-linear combinations of the rows of the generator matrix. Be aware that linear codes over $R = \mathbb{Z}/(2^k)$ may have torsion; that is, nontrivial linear combinations of generators may in fact be zero. In the following examples, the vertical lines in the G_i^E matrices are present only to serve as visual cues for the reader: to the left of the line, the matrix G_i^E agrees with G_i^L.

EXAMPLE 2. Let $R = \mathbb{Z}/(4)$. The generator matrices

$$G_1^L = \begin{pmatrix} 0 & 2 & 0 & 2 & 2 & 2 & 0 \\ 1 & 1 & -1 & -1 & 0 & 2 & 2 \end{pmatrix},$$

$$G_1^E = \left(\begin{array}{ccccccc|c} 0 & 2 & 0 & 2 & 2 & 2 & 0 & 0 \\ 1 & 1 & -1 & -1 & 0 & 2 & 2 & 2 \end{array}\right),$$

both generate linear codes that are isomorphic to $\mathbb{Z}/(2) \oplus \mathbb{Z}/(4)$, with cardinality 8. The code generated by G_1^L has length 7 and constant Lee weight 8, while the code generated by G_1^E has length 8 and constant Euclidean weight 16.

$$G_2^L = \begin{pmatrix} 0 & 0 & 1 & 1 & 1 & 1 & 2 & 2 & -1 & -1 & -1 & -1 & 0 & 2 & 2 \\ 1 & -1 & 0 & 1 & 2 & -1 & 1 & -1 & 0 & 1 & 2 & -1 & 2 & 0 & 2 \end{pmatrix},$$

$$G_2^E = \left(\begin{array}{ccccccccccccccc|ccc} 0 & 0 & 1 & 1 & 1 & 1 & 2 & 2 & -1 & -1 & -1 & -1 & 0 & 2 & 2 & 0 & 2 & 2 \\ 1 & -1 & 0 & 1 & 2 & -1 & 1 & -1 & 0 & 1 & 2 & -1 & 2 & 0 & 2 & 2 & 0 & 2 \end{array}\right).$$

The linear codes generated by G_2^L and G_2^E are both isomorphic to $(\mathbb{Z}/(4))^2$, with cardinality 16. The code generated by G_2^L has length 15 and constant Lee weight 16, while the code generated by G_2^E has length 18 and constant Euclidean weight 32.

EXAMPLE 4. This time, let $R = \mathbb{Z}/(8)$. Set

$$G_3^L = \begin{pmatrix} 0 & 0 & 0 & 0 & 4 & 4 & 4 & 4 & 4 & 4 & 4 & 4 & 0 & 0 & 0 \\ 1 & 3 & -3 & -1 & 0 & 1 & 2 & 3 & 4 & -3 & -2 & -1 & 2 & -2 & 4 \end{pmatrix},$$

$$G_3^E = \left(\begin{array}{ccccccccccccccc|cccc} 0 & 0 & 0 & 0 & 4 & 4 & 4 & 4 & 4 & 4 & 4 & 4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 3 & -3 & -1 & 0 & 1 & 2 & 3 & 4 & -3 & -2 & -1 & 2 & -2 & 4 & 2 & -2 & 4 & 4 \end{array}\right).$$

The linear codes generated by G_3^L and G_3^E are both isomorphic to $\mathbb{Z}/(2) \oplus \mathbb{Z}/(8)$, with cardinality 16. The code generated by G_3^L has length 15 and constant Lee weight 32, while the code generated by G_3^E has length 19 and constant Euclidean weight 128.

4. Equivalence, automorphisms and orbits

Over $R = \mathbb{Z}/(2^k)$, equipped with either Lee or Euclidean weight, two linear codes C, C' in R^n are *equivalent* if there exists a signed permutation transformation of R^n carrying one code to the other. We consider linear codes only up to equivalence.

Note that reduction mod 2^i makes $\mathbb{Z}/(2^i)$ into a module over $R = \mathbb{Z}/(2^k)$, if $i \leq k$.

PROPOSITION 5. *Any linear code C is isomorphic, as an R-module, to a direct sum*

$$C \cong \bigoplus_{i=1}^{k} \left(\mathbb{Z}/(2^i)\right)^{l_i}, \tag{3}$$

for some nonnegative integers $l_1, l_2, \ldots, l_k$.

PROOF. The proof is by induction on k. When $k = 1$, $R = \mathbb{Z}/(2)$ is a field, and the result is classical.

Turn now to a general k. Because C is a module over $\mathbb{Z}/(2^k)$, every element of C has order dividing 2^k. If $x \in C$ has order exactly 2^k, then the submodule Rx generated by x is a free R-module. But R is a quasi-Frobenius ring, so that R is an injective module over itself. Thus the free submodule Rx is a direct summand of C, and $C \cong \mathbb{Z}/(2^k) \oplus V$, for some R-module V. Applying the same argument to V, we split off as large a free module as possible. Thus

$$C \cong \left(\mathbb{Z}/(2^k)\right)^{l_k} \oplus C',$$

for some nonnegative integer l_k and some R-module C', where every element of C' has order dividing 2^{k-1}.

The R-module C' arises from a module over the ring $\mathbb{Z}/(2^{k-1})$ via the change of base rings $\mathbb{Z}/(2^k) \to \mathbb{Z}/(2^{k-1})$. By the induction hypothesis, the module C' splits as in (3), and the result follows. □

To avoid degenerate cases where C is actually a module over a smaller ring $\mathbb{Z}/(2^i)$, we assume from here on that $l_k \geq 1$.

A *linear automorphism* of C is any R-homomorphism $f : C \to C$ which is invertible. Note that this definition does not involve the weight function w, so that f need not be a

is a code automorphism. Denote the group of all linear automorphisms of C by $\mathrm{Aut}(C)$.

The linear automorphism group $\mathrm{Aut}(C)$ acts naturally on C and on $C^\sharp = \mathrm{Hom}_R(C, R)$, the linear dual of C. The action of $\mathrm{Aut}(C)$ then decomposes C and $C^\sharp$ into *orbits*:

$$\mathrm{orb}(x) = \{y : y = f(x), \text{ for some } f \in \mathrm{Aut}(C)\}.$$

EXAMPLE 6. Let $R = \mathbb{Z}/(4)$ and $C \cong \mathbb{Z}/(2) \oplus \mathbb{Z}/(4)$, with elements of C written as columns. There are three nonzero orbits of $\mathrm{Aut}(C)$ in C:

$$\begin{matrix} 0 & 2 & 0 & 2 \\ 1 & 1 & -1 & -1 \end{matrix}', \qquad \begin{matrix} 2 & 2 \\ 0 & 2 \end{matrix}', \qquad \begin{matrix} 0 \\ 2 \end{matrix}.$$

EXAMPLE 7. Let $R = \mathbb{Z}/(4)$ and $C \cong (\mathbb{Z}/(4))^2$. The two nonzero orbits of $\mathrm{Aut}(C)$ in C are

$$\begin{matrix} 0 & 0 & 1 & 1 & 1 & 1 & 2 & 2 & -1 & -1 & -1 & -1 \\ 1 & -1 & 0 & 1 & 2 & -1 & 1 & -1 & 0 & 1 & 2 & -1 \end{matrix}', \qquad \begin{matrix} 0 & 2 & 2 \\ 2 & 0 & 2 \end{matrix}.$$

EXAMPLE 8. This time, let $R = \mathbb{Z}/(8)$ and $C \cong \mathbb{Z}/(2) \oplus \mathbb{Z}/(8)$. The five nonzero orbits are

$$\begin{matrix} 0 & 0 & 0 & 0 & 4 & 4 & 4 & 4 \\ 1 & 3 & -3 & -1 & 1 & 3 & -3 & -1 \end{matrix}', \qquad \begin{matrix} 0 & 0 \\ 2 & -2 \end{matrix}', \qquad \begin{matrix} 4 & 4 \\ 2 & -2 \end{matrix}', \qquad \begin{matrix} 4 & 4 \\ 0 & 4 \end{matrix}', \qquad \begin{matrix} 0 \\ 4 \end{matrix}.$$

5. Orbit structure of constant weight codes

A linear code $C \subset R^n$ can be viewed as an abstract R-module as in (3), equipped with a linear embedding into R^n. The embedding is given by n *coordinate functionals* $\lambda_1, \ldots, \lambda_n \in C^\sharp$. If C has a generator matrix G, then the columns of G are the values of the λ_i evaluated on a set of generators for C. In terms of coordinate functionals, two linear codes of the same length are equivalent if they have the same underlying abstract R-module and the same collection of coordinate functionals, up to ordering and $\pm$ signs.

The main restriction on constant weight codes is that entire orbits of linear functionals must occur as coordinate functionals of C.

THEOREM 9. *Let $C \subset R^n$ be a linear code of constant weight, either Lee or Euclidean weight. If $\lambda \in C^\sharp$ occurs as a coordinate functional of C, then (up to $\pm$ signs) every other linear functional μ in the $\mathrm{Aut}(C)$-orbit of λ also occurs as a coordinate functional of C.*

PROOF. Given μ in the orbit of λ, there exists some $f \in \mathrm{Aut}(C)$ carrying λ to μ. On the other hand, f preserves weight (i.e., $w(f(x)) = w(x)$, for all $x \in C$), since C has constant weight. By the extension theorem [**7**, Theorem 3.1], f extends to a signed permutation automorphism of R^n. Thus $\pm\mu$ is another coordinate functional of C. □

A similar argument shows that $\pm\lambda$ and $\pm\mu$ occur with the same multiplicity.

REMARK 10. We caution the reader that Theorem 9 is a theorem only to the extent that the extension theorem holds for Lee or Euclidean weight. The extension theorem is *not* known in general for rings of the form $R = \mathbb{Z}/(m)$. However, the author has used MAPLE to verify that sufficient conditions for the extension theorem ([**7**, Theorem 3.1]) do hold for $m \leq 256$.

In this section, we use Theorem 9 to prove that, if an abstract R-module C admits *any* constant weight embedding, then C admits such an embedding of minimal length. Moreover, any other constant weight embedding is, up to equivalence, a replication of the minimal one. In Section 7, we show that every abstract R-module C does indeed admit a constant weight embedding.

A linear code of length n can always be viewed as a code of length $n+1$ by adding a zero entry, i.e., by enlarging the set of coordinate functionals $\lambda_1, \ldots, \lambda_n$ to include $\lambda_{n+1} = 0$. We call a linear code *nondegenerate* if it has no zero coordinate functionals.

Let us clarify some terminology mentioned above. An r-fold *replication* of a code C of length n is a new code of length rn having the same coordinate functionals as C, but with each having multiplicity r. In terms of generator matrices, one repeats each column r times.

Before we proceed to the main theorem, we will need some intermediate results. Let $\mathcal{O}$ and $\mathcal{O}^\sharp$ denote the sets of nonzero orbits of $\mathrm{Aut}(C)$ on C and $C^\sharp$, respectively. Let $\mathbb{Q}[\mathcal{O}]$ and $\mathbb{Q}[\mathcal{O}^\sharp]$ be the vector spaces over $\mathbb{Q}$ whose bases consist of the elements of $\mathcal{O}$ and $\mathcal{O}^\sharp$, respectively. These vector spaces can be thought of as the vector spaces of rational-valued functions on $\mathcal{O}$, $\mathcal{O}^\sharp$, respectively. Because of the duality of the actions of $\mathrm{Aut}(C)$ on C and $C^\sharp$, $\mathcal{O}$ and $\mathcal{O}^\sharp$ have the same number of elements, and hence the vector spaces $\mathbb{Q}[\mathcal{O}]$ and $\mathbb{Q}[\mathcal{O}^\sharp]$ have the same dimension.

Next we define a linear mapping $\phi : \mathbb{Q}[\mathcal{O}^\sharp] \to \mathbb{Q}[\mathcal{O}]$. It suffices to describe ϕ on a basis of $\mathbb{Q}[\mathcal{O}^\sharp]$ and extend by linearity. For $\mathrm{orb}(\lambda) \in \mathcal{O}^\sharp$, $\phi(\mathrm{orb}(\lambda))$ will be a rationalvalued function on $\mathcal{O}$. We define

$$(\phi(\mathrm{orb}(\lambda)))(\mathrm{orb}(x)) = \begin{cases} \frac{1}{2}\sum_{\mu \in \mathrm{orb}(\lambda)} a_{\mu(x)}, & \text{if } \lambda \neq -\lambda, \\ \sum_{\mu \in \mathrm{orb}(\lambda)} a_{\mu(x)}, & \text{if } \lambda = -\lambda. \end{cases}$$

The reader will check that this definition is well-defined (in both λ and x). Here, the a_t are the individual element weights that appear in the weight function w; see (2). The sums above are those portions of $w(x)$ which arise from the coordinate functionals in $\mathrm{orb}(\lambda)$, modulo $\pm$ signs.

REMARK 11. This definition of ϕ works for any weight function, as long as the sums involved are rational. In the case of the first notion of Euclidean weight, Remark 1, the reader will check that, even though $a_t = 2 - 2\cos(2\pi t/m)$ is generally irrational, the sums above are still rational.

PROPOSITION 12. *The linear mapping $\phi : \mathbb{Q}[\mathcal{O}^\sharp] \to \mathbb{Q}[\mathcal{O}]$ is an isomorphism.*

PROOF. Since the vector spaces have the same dimension, it suffices to show that ϕ is injective. To that end, first examine the special case where $p, q \in \mathbb{Q}[\mathcal{O}^\sharp]$ actually have nonnegative integral coefficients. Then p, q describe two linear codes, using as coordinate functionals the functionals in the various orbits in $\mathcal{O}^\sharp$, modulo $\pm$ signs, with multiplicities given by p, q. Then $\phi(p) = \phi(q)$ says that the two codes have the same weights. By the extension theorem [**7**], the codes are equivalent, hence $p = q$.

The general case follows from this special case by clearing denominators and adding sufficiently large integral combinations to both p, q. That is, find an integer N and an integral $r \in \mathbb{Q}[\mathcal{O}^\sharp]$ such that both $Np + r$ and $Nq + r$ have nonnegative integral coefficients. Then $\phi(p) = \phi(q)$ implies $\phi(Np + r) = \phi(Nq + r)$. The special case applies, and $Np + r = Nq + r$, from which $p = q$ follows. □

THEOREM 13. *Let C be any R-module of the form (3), and suppose that C admits a constant weight embedding. Then C admits a constant weight embedding of minimal*

lence, a replication of the constant weight embedding of minimal length.

PROOF. If C admits a constant weight embedding with constant weight L, then Theorem 9 says that the embedding is described by some $p \in \mathbb{Q}[\mathcal{O}^\sharp]$ with nonnegative integral coefficients. The constant weight condition says that $(\phi(p))(\mathrm{orb}(x)) = L$, for every $\mathrm{orb}(x) \in \mathcal{O}$. Thus $\phi(p)$ lies on the one-dimensional subspace $\mathcal{L}$ of $\mathbb{Q}[\mathcal{O}]$ where all the coefficients are equal.

The inverse image of $\mathcal{L}$ in $\mathbb{Q}[\mathcal{O}^\sharp]$ is also one-dimensional. By clearing demoninators and factoring out any common factors, this one-dimensional subspace has a basis whose coefficients are relatively prime integers. Any other integral element of this one-dimensional subspace will be an integral multiple of the basis element. (This is the replication result.)

The only problem is if the basis element has some negative coefficients. This is the reason we assume the existence of some constant weight embedding: this guarantees nonnegative coefficients. □

7. An existence result

All that remains is to show that constant weight embeddings exist. In the Lee weight case, Carlet gives the answer. We include a proof which illustrates, in the simpler Lee setting, the techniques which will be used in the Euclidean case.

THEOREM 14 (Carlet [**3**]). *Let C be any module over $R = \mathbb{Z}/(2^k)$ of the form (3). Then the code whose coordinate functionals consist of all the nonzero linear functionals on C has constant Lee weight.*

This code has cardinality $|C| = 2^{l_1+2l_2+\cdots+kl_k}$ and length equal to $|C| - 1$. Every nonzero codeword has Lee weight $2^{k-2}|C|$.

PROOF. Take any nonzero $x \in C$. Since the coordinate functionals consist of all the nonzero linear functionals on C, we have

$$w(x) = \sum_{\lambda \in C^\sharp} a_{\lambda(x)}.$$

There is no harm in including $\lambda = 0$ in the sum, since $a_0 = 0$.

The linear functional $\check{x} : C^\sharp \to R$, $\lambda \mapsto \lambda(x)$, has image $\mathrm{im}(\check{x})$ which is some nonzero ideal $(2^\mu) \subset R$. Each $r \in \mathrm{im}(\check{x})$ is hit equally often under $\check{x}$, namely

$$|\ker(\check{x})| = \frac{|C^\sharp|}{|\mathrm{im}(\check{x})|} = \frac{|C^\sharp|}{|(2^\mu)|} = \frac{|C|}{2^{k-\mu}}$$

times. Thus

$$w(x) = \frac{|C|}{2^{k-\mu}} \sum_{r \in (2^\mu)} a_r.$$

It is straight forward to verify that, for Lee weight,

$$\sum_{r \in (2^\mu)} a_r = 2^{2k-2-\mu}.$$

Thus $w(x) = 2^{k-2}|C|$, as claimed. □

is as in (3). Using the rank numbers $l_1, \ldots, l_k$, define

$$\begin{aligned}
&& e_0 &= 1 \\
d_1 &= l_1 + l_2 + \cdots + l_k - 1 && e_1 = d_1 \\
d_2 &= \quad l_2 + \cdots + l_k - 1 && e_2 = d_1 + d_2 \\
&\vdots && \vdots \\
d_{k-1} &= \quad l_{k-1} + l_k - 1 && e_{k-1} = d_1 + d_2 + \cdots + d_{k-1} \\
d_k &= \quad l_k - 1 && e_k = d_1 + d_2 + \cdots + d_{k-1} + d_k
\end{aligned}$$

The R-module $C^\sharp$ admits a filtration

$$C^\sharp \supset 2C^\sharp \supset 4C^\sharp \supset \cdots \supset 2^{k-1}C^\sharp \supset 2^k C^\sharp = 0.$$

For $\lambda \in C^\sharp$, let $\nu(\lambda)$ be the largest exponent such that $\lambda \in 2^{\nu(\lambda)}C^\sharp$. For nonzero λ, $\nu(\lambda) \leq k-1$.

THEOREM 15. *Let C be any module over $R = \mathbb{Z}/(2^k)$ of the form (3), with $l_k \geq 1$. Then there exists a linear embedding of C with constant Euclidean weight. Every nonzero linear functional $\lambda \in C^\sharp$ appears as a coordinate functional with multiplicity*

$$m_{\nu(\lambda)} = \sum_{i=0}^{\nu(\lambda)} 2^{e_i}.$$

The cardinality of C is $|C| = 2^{l_1 + 2l_2 + \cdots + kl_k}$, and its length is

$$\frac{|C|}{2^{k-1}}\left(3 \cdot 2^{k-1} - 1\right) - m_{k-1}. \tag{4}$$

Every nonzero element of C has Euclidean weight $2^{2k-2}|C|$.

To obtain the minimal length embedding, one must, in general, divide each of the multiplicities $m_{\nu(\lambda)}$ by 2. The only exception is when $C \cong \mathbb{Z}/(2^k)$ itself. The length and constant weight of the minimal length embedding scale appropriately.

Since we assume $l_k \geq 1$, 2^k divides $|C|$, and (4) is an integer.

PROOF. Take any nonzero $x \in C$. Because each $\lambda \in C^\sharp$ occurs as a coordinate functional with multiplicity $m_{\nu(\lambda)}$, we have

$$w(x) = \sum_{\lambda \in C^\sharp} m_{\nu(\lambda)} a_{\lambda(x)}. \tag{5}$$

Since $a_0 = 0$, there is no harm in including $\lambda = 0$ in the sum. Using the definition of $m_{\nu(\lambda)}$ and the fact that $2^{\nu(\lambda)}C^\sharp \subset 2^{\nu(\lambda)-1}C^\sharp \subset \cdots \subset C^\sharp$, we can rewrite (5) as

$$w(x) = \sum_{j=0}^{k-1} 2^{e_j} \sum_{\lambda \in 2^j C^\sharp} a_{\lambda(x)}. \tag{6}$$

Now consider the linear functional $\check{x} : 2^j C^\sharp \to R$, $\lambda \mapsto \lambda(x)$. Suppose x has order 2^i; that is, $2^i x = 0$, but $2^{i-1}x \neq 0$. If $i \leq j$, then the functional $\check{x}$ is zero. When $i > j$, the image $\mathrm{im}(\check{x}) = \check{x}(2^j C^\sharp) = (2^{k-i+j})$, of order $|\mathrm{im}(\check{x})| = 2^{i-j}$. In the latter case, every $r \in \mathrm{im}(\check{x})$ is hit equally often by $\check{x}$, namely

$$|\ker(\check{x})| = \frac{|2^j C^\sharp|}{|\mathrm{im}(\check{x})|} = 2^{l_{j+1} + 2l_{j+2} + \cdots + (k-j)l_k - i + j}$$

$$\sum_{r\in(2^\mu)} a_r = \frac{1}{3}\,2^{k+\mu-1}\left(2^{2k-2\mu-1}+1\right). \tag{7}$$

Remembering that x has order 2^i and using $\mu = k-i+j$ in (7), we conclude that

$$\sum_{\lambda\in 2^jC^\natural} a_{\lambda(x)} = \begin{cases} 0, & i\le j,\\ \frac{1}{3}\,2^{l_{j+1}+2l_{j+2}+\cdots+(k-j)l_k}\left(1+2^{-2i+2j+1}\right)2^{2k-2}, & i>j. \end{cases} \tag{8}$$

By substituting (8) into (6), we rewrite (6) as

$$w(x) = \sum_{j=0}^{i-1} \frac{1}{3}\,2^{e_j+l_{j+1}+2l_{j+2}+\cdots+(k-j)l_k}\left(1+2^{-2i+2j+1}\right)2^{2k-2}. \tag{9}$$

Observe that the complicated exponent in (9) simplifies to

$$e_j + l_{j+1} + 2l_{j+2} + \cdots + (k-j)l_k = \begin{cases} 1+\sum_{h=1}^k hl_h, & j=0,\\ -j+\sum_{h=1}^k hl_h, & j>0. \end{cases} \tag{10}$$

Since $\log_2|C| = \sum_{h=1}^k hl_h$, (9) simplifies to

$$w(x) = \frac{2}{3}|C|\left(1+2^{-2i+1}\right)2^{2k-2} + \sum_{j=1}^{i-1}\frac{1}{3}|C|\,2^{-j}\left(1+2^{-2i+2j+1}\right)2^{2k-2}.$$

By summing the geometric series and simplifying, this last expression simplifies to

$$w(x) = 2^{2k-2}|C|,$$

as claimed.

The remaining claims of the theorem can be verified easily. □

The reader will check that the examples of Section 3 are of the form described in the theorems above. In the Euclidean case, all the examples in Section 3 have minimal length.

References

[1] A. Bonisoli, *Every equidistant linear code is a sequence of dual Hamming codes*, Ars Combin. **18** (1984), 181–186.

[2] A. Bonnecaze, P. Solé, and A. R. Calderbank, *Quaternary quadratic residue codes and unimodular lattices*, IEEE Trans. Inform. Theory **41** (1995), 366–377.

[3] C. Carlet, *One-weight $\mathbb{Z}_4$-linear codes*, preprint, 1998.

[4] A. R. Hammons, Jr., P. V. Kumar, A. R. Calderbank, N. J. A. Sloane, and P. Solé, *The $\mathbb{Z}_4$-linearity of Kerdock, Preparata, Goethals, and related codes*, IEEE Trans. Inform. Theory **40** (1994), 301–319.

[5] H. N. Ward, *A bound for divisible codes*, IEEE Trans. Inform. Theory **38** (1992), 191–194.

[6] H. N. Ward and J. A. Wood, *Characters and the equivalence of codes*, J. Combin. Theory, series A **73** (1996), 348–352.

[7] J. A. Wood, *Weight functions and the extension theorem for linear codes over finite rings*, Finite Fields: Theory, Applications and Algorithms (R. C. Mullin and G. L. Mullen, eds.), Contemp. Math., vol. 225, Amer. Math. Soc., Providence, RI, 1999, pp. 231–243.

URL: `http://www.calumet.purdue.edu/public/math/wood/`